Challenges in Disaster Mitigation of Large Infrastructure by Engineering Design

Baidurya Bhattacharya
Indian Institute of Technology Kharagpur

Introduction

Infrastructure refers to the basic framework that underlies and holds together a complex system. A country or a region depends on its civil, communication, military, financial and other infrastructure to function and serve its citizens. This talk is about civil infrastructure systems i.e., the built environment which includes the transportation, power, water etc. infrastructure systems. An infrastructure has many interconnected parts, working together to provide a desired solution to society. For example, the transportation infrastructure of a nation is composed of its port, airport, road, bridge, air, rail etc. systems. Large scale industrialization started in the nineteenth century and the word infrastructure came into English less than a hundred years ago. With the harnessing of steam, electricity and explosives, together with the ability to make new and better materials, humans had the ability to span distance and reduce communication time at a scale not possible before.

Evolution of engineering design

Building complex systems does not happen by chance or in a vacuum. Up until the middle of the 19th century, engineering, be it making a castle, a bridge or a watch, was mostly an art – it was conceived by intuition, designed by experience, performed often by one very talented individual, expected to last long and put up by factor of safety. Testing, repeatability, collaboration or optimization was not of primary concern. The art aspect is still very much central to engineering, for one cannot build something if one cannot imagine it, but rigorous science has become the bedrock of modern engineering. The modern engineer has made society more democratic: more people have access to what once belonged only to kings – be it indoor plumbing, indoor illumination, high speed travel or instant communication. In the process, modern engineering has also become a hugely complex and demanding endeavour – better and cheaper products must be produced at an ever increasing pace while they must continue to be safe and reliable. Such demands require constant innovation and teamwork involving hundreds or thousands of professionals often spread over a large geographical area.

When building something, the engineer always knows that something might go wrong with it, and his/her solution might not work the way it is supposed to. Failure might mean economic/human/environmental loss to the owner and society on the one hand, and, on the other, loss of business and reputation, penalty, and, in ancient times, even death for the engineer. Factors of safety have been the traditional means to preventing such undesirable occurrences.

Factors of safety work well when the system is mature and pace of innovation is slow, overdesign is not a dealbreaker, and knowledge of system performance – particularly under trying conditions – is limited. Traditional design is component based. The engineer designs the system component by component for

ordinary demands, then makes each component safer by a comfortable factor, and hopes that the system will hold good under extraordinary demands. As stated above, this strategy works when the technology is mature, cost is not much of a concern, and the system is not expected to perform under extraordinary or exceptional conditions.

Managing failure

But, systems do fail. And big systems fail in big ways, causing big losses. And if they fail, they often fail in hitherto unknown ways. If the country's financial system is too big to fail, necessitating important elements of that infrastructure to be propped up to prevent collapse of the entire system, so is any one among the country's civil infrastructure – its water supply, power, transportation, building and other infrastructure systems. The difference is, important elements of the civil infrastructure system, such as a large bridge, a nuclear power plant or an airport, if they fail, cannot be propped up or replaced immediately. It can take months or even years for the system to come back up to full functionality. Remember the still unfinished levee system of New Orleans after Katrina in 2005, the unfolding of Fukushima-Daiichi nuclear meltdown of 2011, cleanup after the Deep Horizon blowup and oilspill in Gulf of Mexico in 2010, the aftermath of Hurricane Aila in West Bengal and Bangladesh in 2009, the destruction after the Indian Ocean tsunami of 2004 etc.

So it is imperative that large infrastructure systems be designed not only to provide full functionality under normal conditions, they must also be able to absorb limited damages without tripping, be able to provide essential services after a major strike, and have the ability to come back up online within a reasonable time after being hit by a disaster. These are very demanding requirements and rather idealistic in nature. However, we must evaluate our existing as well as our upcoming infrastructure systems against these expansive desiderata in precise measurable ways, if we wish to have our engineering infrastructure serve us in normal times as well as in times of crises.

Performance expectations and how to achieve them

The first task in designing an infrastructure system, then, is to spell out our expectations – its performance requirements – under a range of system conditions, e.g., normal, partially damaged and severely damaged. The damage states must be defined in precise measurable terms.

Once the performance requirements are understood, the designer must make a comprehensive survey of the hazards that are likely to befall the system during its design life. Different performance levels should generally be evaluated against different types and/or magnitudes of hazard. Man-made hazards are different from natural hazards in that the former are inflicted by an intelligent agent to cause harm, and thus may cause damage disproportionate to the extent and scale of attack. The engineer also has to define the so-called design envelope in order to admit that it is either too costly or technically impossible or both to meet hazard scenarios beyond this envelop.

The third task is to define the confidence or reliability with which the system must perform its intended functions subjected to the appropriate hazards. Uncertainties abound in any engineering activity, and the uncertainties about a large infrastructural system are significant indeed. There are uncertainties

about the occurrence and magnitudes of the hazards, the loads they cause on the system, the strength of each element of the system, the manner in which these elements influence and interact with each other, and finally in the mathematical model s with which we evaluate the hazards and system performance. Under such myriad uncertainties, it is clear that the system can meet its requirements not every time; the frequency or confidence with which it does so must be evaluated probabilistically and compared to predefined target. These target reliabilities/availabilities are not in the purview of the engineer alone, they need to be set by engineers, economists and policy makers, and must take into account the consequences of failure, the cost of mitigation measures, and the perception of risk from the failed infrastructure by members of the public.

Current challenges

Once these three tasks are in place, design of the infrastructure system can proceed in the usual iterative manner and it is the responsibility of the designer to provide the most economical solution for the design. It can so happen that in case of severe system damage under an extreme hazard, the system can meet its performance requirements with the required reliability only if adequate post-disaster management activities are factored into the design.

At the current state of the art, the impediments to realizing the ideal solution described above relate to three major aspects: the first to do with uncertainty, the second in regard to modeling of the system, and the third to do with risk communication.

1. **Uncertainty quantification.** There is lack of complete knowledge about the input, i.e., the future hazards and the future demands, to the system. For hazards that arise out of extremes of geophysical processes, how does one reconcile their spatio-temproal scales that are orders of magnitude larger than those of the engineering systems? How does uncertainty in the input propagate through a complex system? How accurately is it possible to predict the state/output of a complex system in the face of significant uncertainty in the input and the model? How are uncertainties arising from human intervention, human error and public behaviour going to affect the response of the system when disaster strikes?

2. **System level model.** It is comparatively easy to model a system in its intact form operating under normal conditions. The model of the system in severely damaged or in near failure conditions becomes inaccurate and cannot be verified against experimental data. How much is the error in the system model itself? Important system failure modes and weak progressive failure sequences may be missed. It is relatively easy to model dependence among events if they are causally related, but associative dependence is more difficult and easy to miss which might give a false sense of safety through redundancy. If the system is instrumented, how can the sensed data under normal conditions, and those under damaged conditions, be used to estimate the extent of damage, and to direct disaster response operations?

3. **Risk communication.** How much risk to life, property and the environment is society willing to accept for the benefits that it gets from the infrastructure, if it fails? How much money is it willing to spend to mitigate an additional unit of risk? What failure costs are to be taken into

account, and which are to be kept out? What is the value of natural beauty that is threatened by a disaster? These questions directly affect the reliability/availability to which the infrastructure system needs to be designed. There may be a large difference between the actual risk of failure of a system, and the risk perceived by the public. How is the proper risk to be communicated? Society's tolerable risk to an activity may change with time: how is one to keep up with it?